US005805712A

United States Patent [19]

Davis

[11] Patent Number: 5,805,712

[45] Date of Patent: Sep. 8, 1998

[54] **APPARATUS AND METHOD FOR PROVIDING SECURED COMMUNICATIONS**

[75] Inventor: **Derek L. Davis**, Phoenix, Ariz.

[73] Assignee: **Intel Corporation**, Santa Clara, Calif.

[21] Appl. No.: **578,177**

[22] Filed: **Dec. 29, 1995**

Related U.S. Application Data

[63] Continuation of Ser. No. 251,486, May 31, 1994, Pat. No. 5,539,828.

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/50**; 380/4; 380/23; 380/25; 380/30; 380/44; 380/46; 380/49; 380/52

[58] **Field of Search** 380/4, 21, 23, 380/25, 29, 30, 44, 46, 49, 50, 9, 52, 59

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,611,293	10/1971	Constable et al. .	
3,806,874	4/1974	Ehrat .	
4,092,524	5/1978	Moreno	235/419
4,204,113	5/1980	Giraud et al.	235/375
4,215,421	7/1980	Giraud .	
4,234,932	11/1980	Gorgens .	
4,271,482	6/1981	Giraud .	
4,310,720	1/1982	Check, Jr. .	
4,467,139	8/1984	Mollier .	
4,471,216	9/1984	Herve	235/380
4,544,833	10/1985	Ugon	235/379
4,549,075	10/1985	Saada et al.	235/380
4,638,120	1/1987	Herve .	
4,656,342	4/1987	Ugon	235/379

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

0624-014-2	4/1994	European Pat. Off. .
69 29737	8/1969	France .
73 12850	10/1973	France .
75 14808	5/1975	France .
77 07322	3/1977	France .

(List continued on next page.)

OTHER PUBLICATIONS

"Cryptographic Identification Methods for Smart Cards in the Process of Standardization", *IEEE Communications Magazine* vol. 29, No. 6, (Jun. 1991) pp. 42–48.

Guillou, L.: "Smart Cards and Conditional Access" in Advances in Cryptology—Proceedings of EUROCRYPT 84; T. Beth, N. Cot and I. Ingemarsson (Eds) Springer–Verlag, 1985, pp. 480–490.

Rankine, G.: "Thomas—A complete Single Chip RSA Device" in Advances in Cryptology—Proceedings of CRYPTO 86; A.M. Odlyzko (Ed), Springer–Verlag, 1987, pp. 480–487.

Struif, B.: "The Use of Chipcards for Electronic Signatures and Encryption" in Proceedings of the 1989 Conference on VLSI and Computer Peripherals, IEEE Computer Society Press, 1989, pp. 4/155–4/158.

Dussé, S.R. & B.S. Kaliski: "A Cryptograohic Library for the Motorola DSP56000" in Advances in Cryptology—Proceedings of EUROCRYPT 90, I.M. Damgård (Ed), Springer–Berlag, 1991, pp. 230–244.

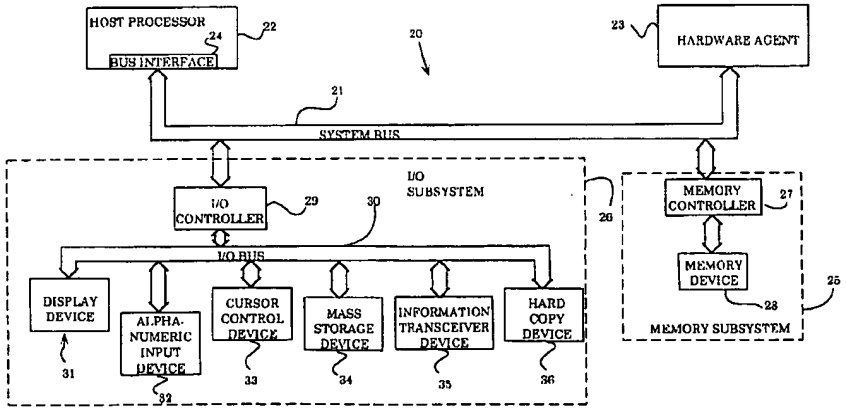
Primary Examiner—Bernarr E. Gregory

Attorney, Agent, or Firm—Blakely, Sokoloff, Taylor & Zafman

[57] **ABSTRACT**

A semiconductor device used to store encryption/decryption keys at manufacture in combination with digital certificates to ensure secured communications between the semiconductor device and another device. The semiconductor device comprising (i) a non-volatile memory capable of storing the encryption/decryption keys and at least one digital certificate, (ii) an internal memory capable of temporarily storing information input into the semiconductor device from the other device and possibly encryption and decryption algorithms, (iii) a processor for processing the information and (iv) a random number generator for generating the encryption/decryption keys completely internal to the semiconductor device.

29 Claims, 8 Drawing Sheets



U.S. PATENT DOCUMENTS

4,656,474	4/1987	Mollier et al.	380/23
4,807,288	2/1989	Ugon et al.	380/30
4,811,393	3/1989	Hazard	380/21
4,825,052	4/1989	Chemin et al.	235/380
4,907,270	3/1990	Hazard	380/23
4,907,272	3/1990	Hazard et al.	380/23
4,910,774	3/1990	Barakat	380/23
5,068,894	11/1991	Hoppe	380/23
5,140,634	8/1992	Guilliu et al.	380/23
5,153,581	10/1992	Hazard .	
5,191,193	3/1993	Le Roux	235/379
5,218,559	6/1993	Angebaud et al.	364/717
5,218,637	6/1993	Angebaud et al.	380/23

FOREIGN PATENT DOCUMENTS

77 16098	5/1977	France .	
77 17436	6/1977	France .	
77 28049	9/1977	France .	
79 08261	4/1979	France .	
79 22033	9/1979	France .	
79 27705	11/1979	France .	
80 04701	3/1980	France .	
80 07912	4/1980	France .	
81 06396	3/1981	France .	
82 08405	5/1982	France .	
82 12021	7/1982	France .	
82 20052	11/1982	France .	
83 00884	1/1983	France .	
84 06221	4/1984	France .	
85 19502	12/1985	France .	
86 08654	6/1986	France .	
86 10206	7/1986	France .	
86 10209	7/1986	France .	
86 10416	7/1986	France .	
87 07093	5/1987	France .	
87 09794	7/1987	France .	
87 12366	9/1987	France .	
89 11113	8/1989	France .	
89 13449	10/1989	France .	
90 07228	6/1990	France .	
91 00440	1/1991	France .	
91 10886	9/1991	France .	
91 16008	12/1991	France .	
92 13726	11/1992	France .	
92 15915	12/1992	France .	
93 11722	10/1993	France .	
93 14466	12/1993	France .	
93 15879	12/1993	France .	
94 01645	2/1994	France .	
94 03773	3/1994	France .	
3410937	10/1985	Germany	G09C 1/00
2154344	9/1985	United Kingdom	G06F 12/14
A-90/02456	3/1990	WIPO .	

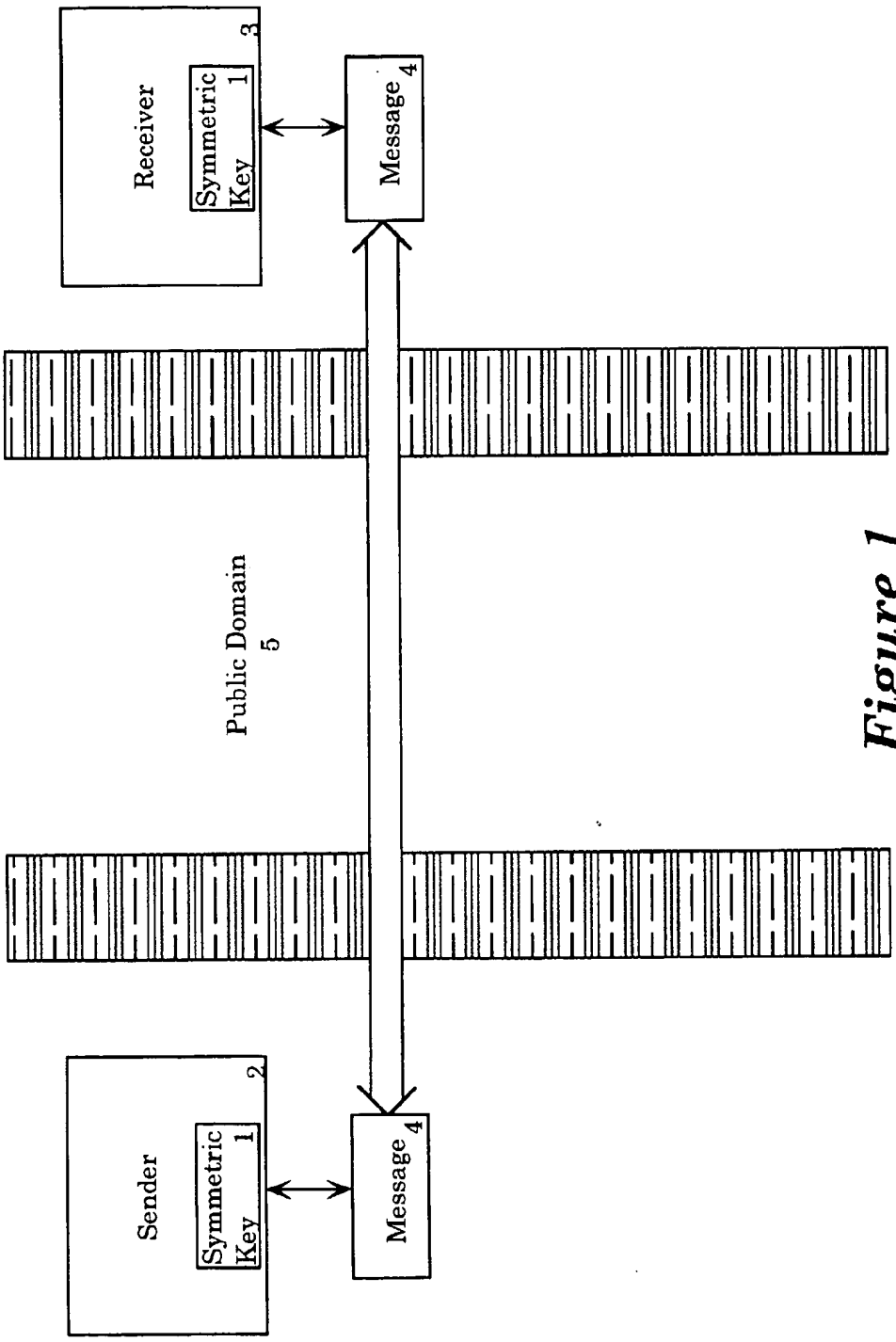


Figure 1
Prior Art

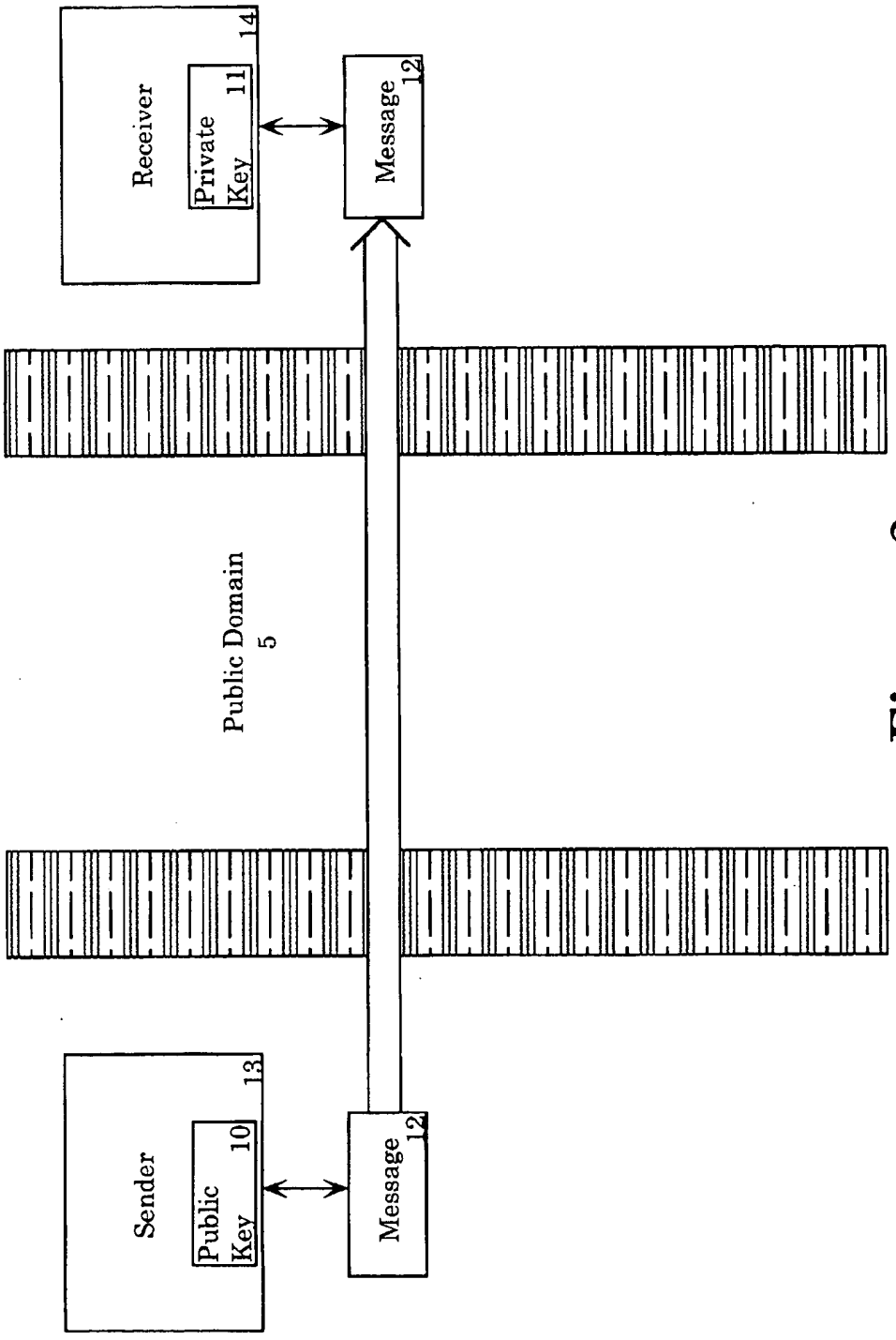


Figure 2
Prior Art

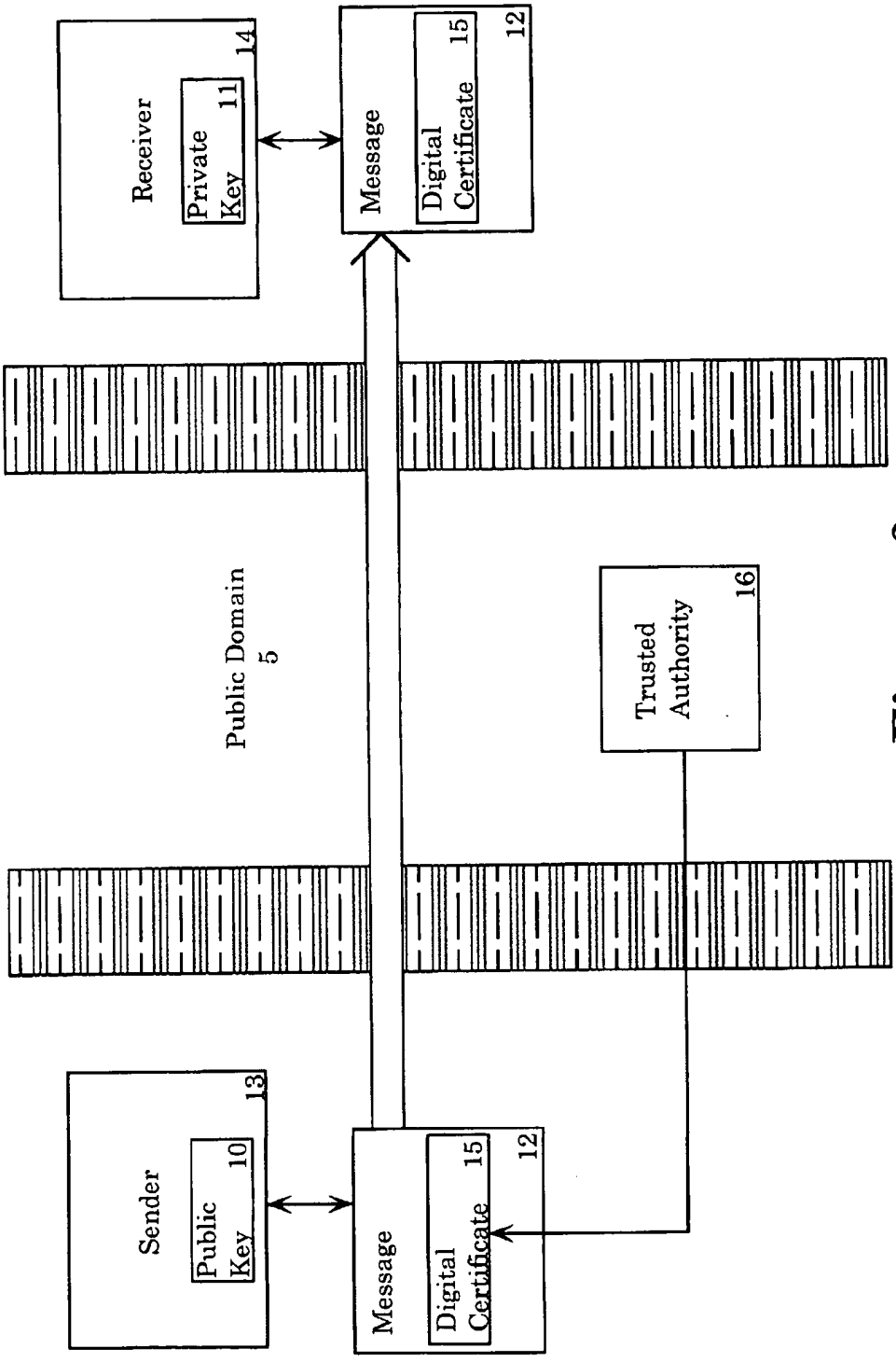


Figure 3
Prior Art

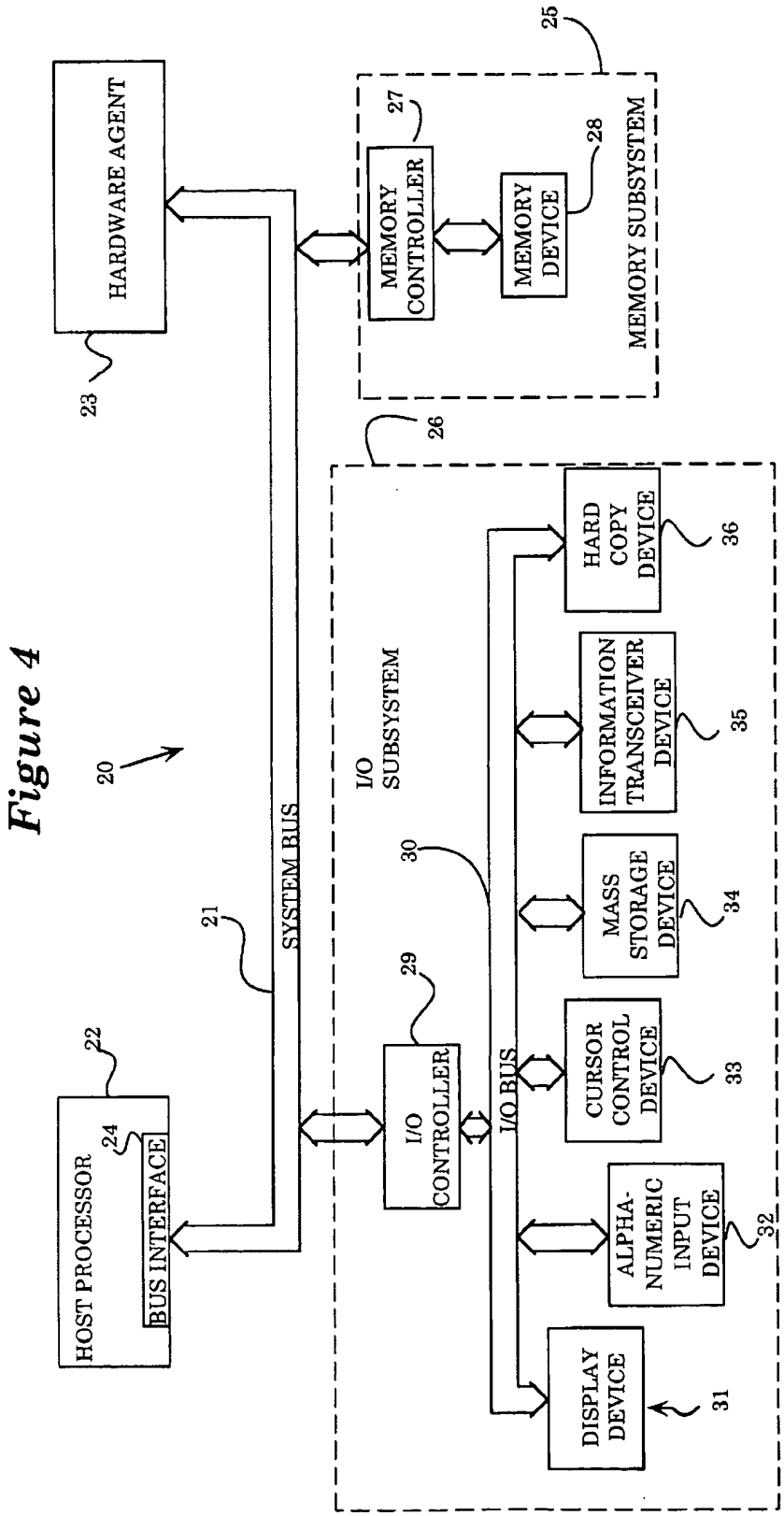

HARDWARE AGENT
23
25
MEMORY SUBSYSTEM
MEMORY CONTROLLER
27
MEMORY DEVICE
28
26
I/O SUBSYSTEM
HARD COPY DEVICE
36
INFORMATION TRANSCEIVER DEVICE
35
MASS STORAGE DEVICE
34
CURSOR CONTROL DEVICE
33
ALPHA-NUMERIC INPUT DEVICE
32
DISPLAY DEVICE
31
30
I/O BUS
29
I/O CONTROLLER
SYSTEM BUS
21
20
22
HOST PROCESSOR
24
BUS INTERFACE

Figure 4

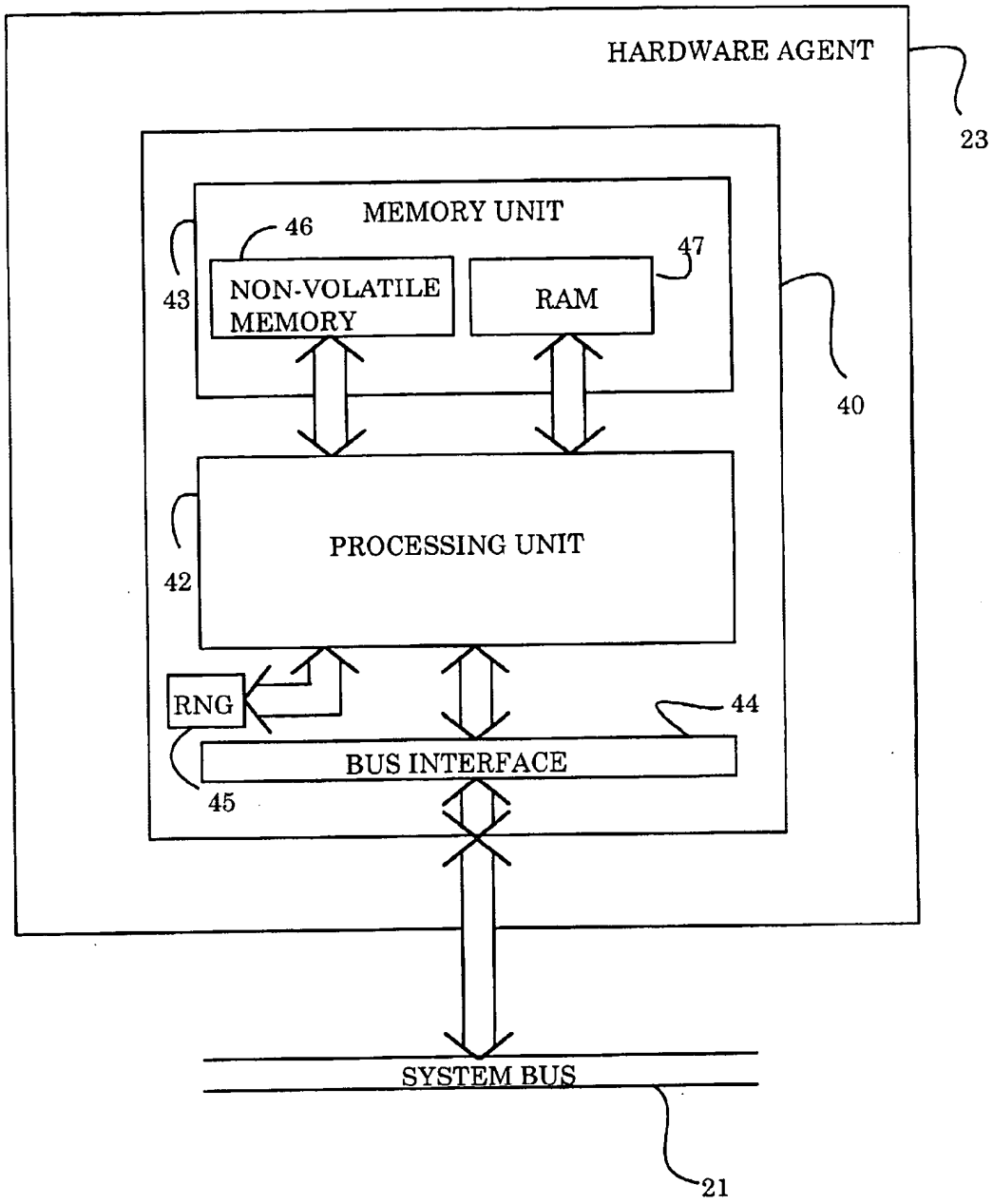

HARDWARE AGENT
23
MEMORY UNIT
46
47
43
NON-VOLATILE MEMORY
RAM
40
PROCESSING UNIT
42
RNG
44
BUS INTERFACE
45
SYSTEM BUS
21

Figure 5

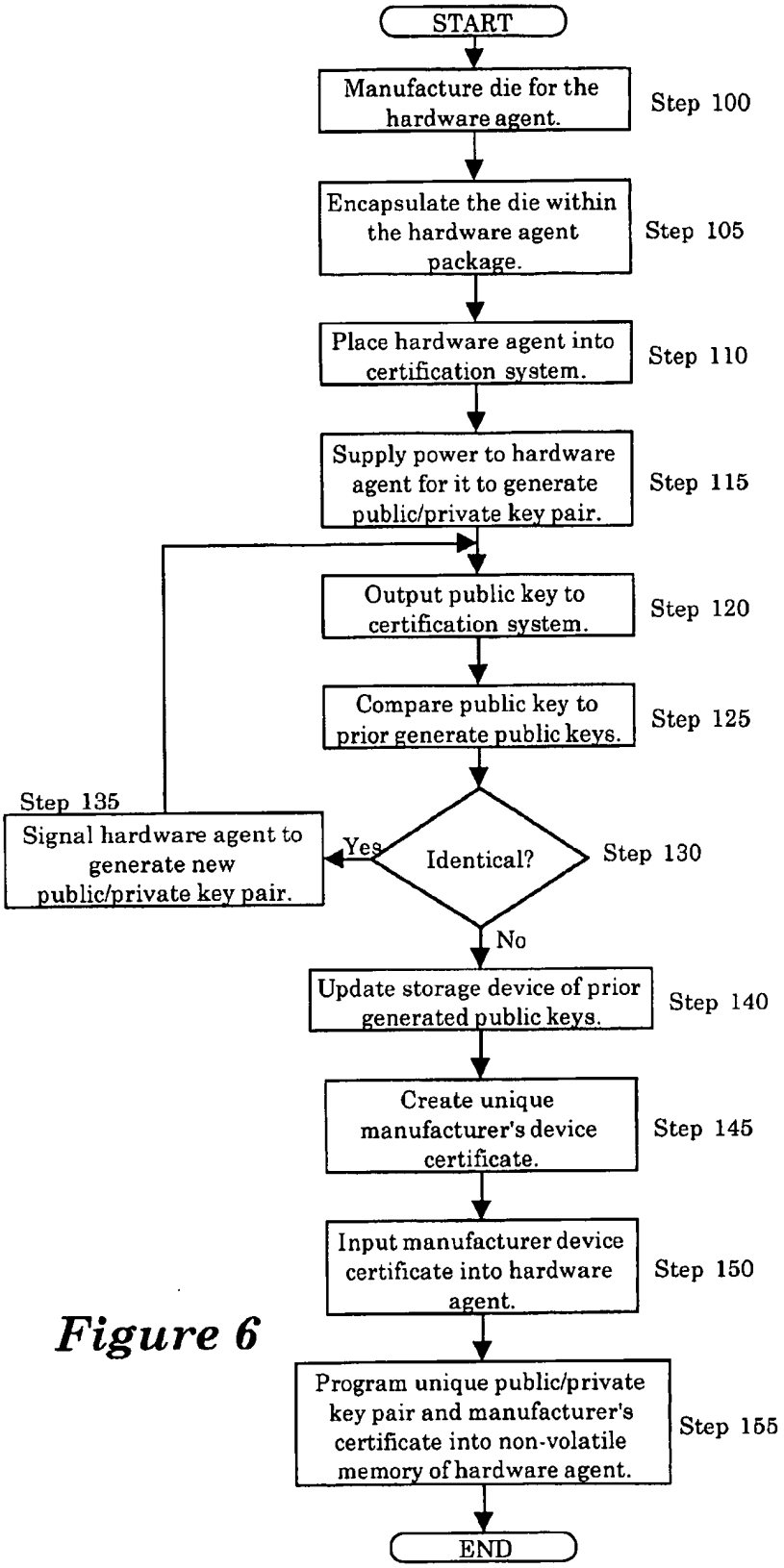

START
Manufacture die for the hardware agent.
Step 100
Encapsulate the die within the hardware agent package.
Step 105
Place hardware agent into certification system.
Step 110
Supply power to hardware agent for it to generate public/private key pair.
Step 115
Output public key to certification system.
Step 120
Compare public key to prior generate public keys.
Step 125
Identical?
Step 130
Yes
Step 135
Signal hardware agent to generate new public/private key pair.
No
Update storage device of prior generated public keys.
Step 140
Create unique manufacturer's device certificate.
Step 145
Input manufacturer device certificate into hardware agent.
Step 150
Program unique public/private key pair and manufacturer's certificate into non-volatile memory of hardware agent.
Step 155
END

Figure 6

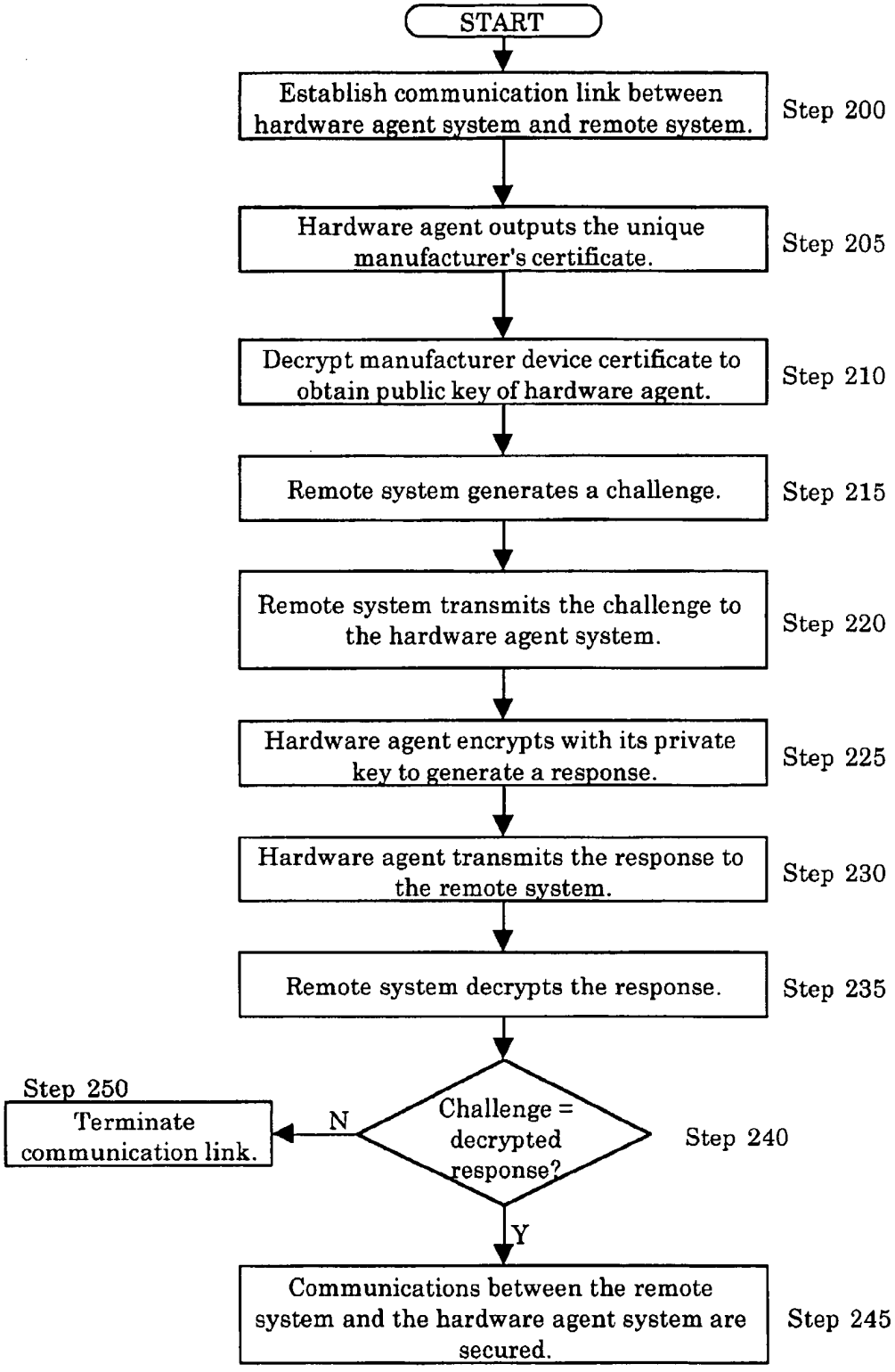

START
Establish communication link between hardware agent system and remote system.
Step 200
Hardware agent outputs the unique manufacturer's certificate.
Step 205
Decrypt manufacturer device certificate to obtain public key of hardware agent.
Step 210
Remote system generates a challenge.
Step 215
Remote system transmits the challenge to the hardware agent system.
Step 220
Hardware agent encrypts with its private key to generate a response.
Step 225
Hardware agent transmits the response to the remote system.
Step 230
Remote system decrypts the response.
Step 235
Challenge = decrypted response?
Step 240
N
Step 250
Terminate communication link.
Y
Communications between the remote system and the hardware agent system are secured.
Step 245

Figure 7

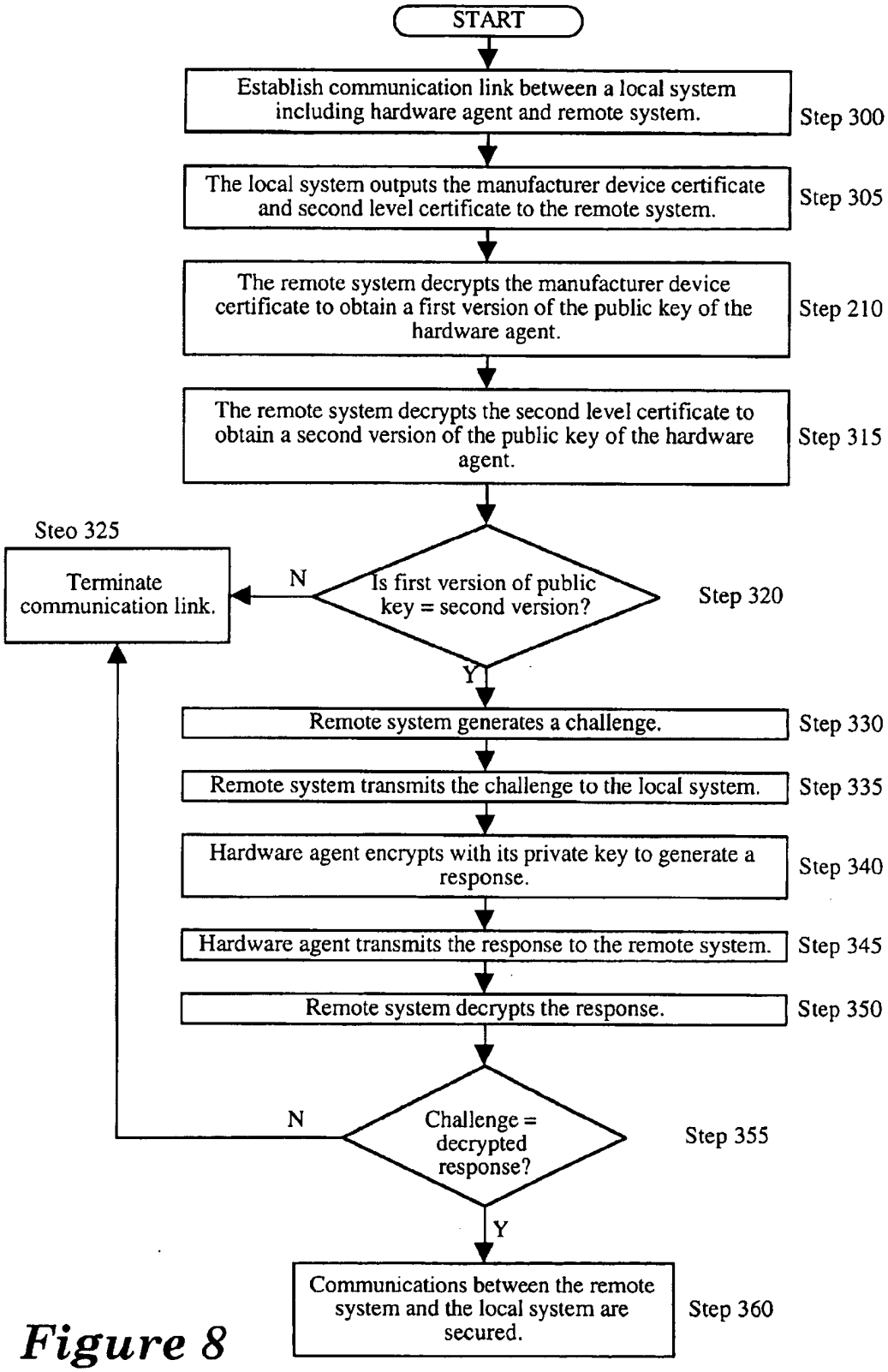

START
Establish communication link between a local system including hardware agent and remote system.
Step 300
The local system outputs the manufacturer device certificate and second level certificate to the remote system.
Step 305
The remote system decrypts the manufacturer device certificate to obtain a first version of the public key of the hardware agent.
Step 210
The remote system decrypts the second level certificate to obtain a second version of the public key of the hardware agent.
Step 315
Steo 325
Terminate communication link.
N
Is first version of public key = second version?
Step 320
Y
Remote system generates a challenge.
Step 330
Remote system transmits the challenge to the local system.
Step 335
Hardware agent encrypts with its private key to generate a response.
Step 340
Hardware agent transmits the response to the remote system.
Step 345
Remote system decrypts the response.
Step 350
N
Challenge = decrypted response?
Step 355
Y
Communications between the remote system and the local system are secured.
Step 360

Figure 8

APPARATUS AND METHOD FOR PROVIDING SECURED COMMUNICATIONS

This application is a continuation of application Ser. No. 08/251,486, filed May 31, 1994, now U.S. Pat. No. 5,539,828.

CROSS-REFERENCES TO RELATED APPLICATIONS

The named inventor of the present application has filed a number of copending U.S. patent applications of which the following have matured into U.S. patents: "Roving Software License For A Hardware Agent" (U.S. Pat. No. 5,473,692), and "A Method For Providing A Roving Software License in A Hardware Agent-Based System" (U.S. Pat. No. 5,568,552). These patents are owned by the same assignee of the present application.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an apparatus and method for data security. More particularity, the present invention relates to a semiconductor device storing encryption/decryption keys at manufacture and/or subsequent to manufacture to ensure secured communications between a system incorporating a cryptographic semiconductor device and a device in remote communications with the system.

2. Art Related to the Invention

In today's society, it is becoming more and more desirable to transmit digital information from one location to another in a manner which is clear and unambiguous to a legitimate receiver, but incomprehensible to any illegitimate recipients. Accordingly, such information is typically encrypted by a software application executing some predetermined encryption algorithm and is transmitted to the legitimate receiver in encrypted form. The legitimate receiver then decrypts the transmitted information for use. This encryption/decryption transmission process is commonly used in governmental applications as well as for commercial applications where sensitive information is being transmitted.

Often, encryption/decryption of information is accomplished through symmetric key cryptography as shown in FIG. 1. In symmetric key cryptography, an identical key **1** (i.e., a data string commonly referred to as a "symmetric key") is used by both a legitimate sender **2** and a legitimate receiver **3** to encrypt and decrypt a message **4** (i.e., information) being transmitted between the sender **2** and receiver **3**. Such encryption and decryption is performed through well-known conventional algorithms such as Riverst, Shamir, and Adleman (RSA) and/or Data Encryption Standard (DES), and transmitted in encrypted form through a public domain **5** such as a conventional network, telephone lines, etc.

Although symmetric key cryptography is computationally simple, it requires complex key management. Basically, each sender needs a different symmetric key to communicate with each legitimate receiver, thereby making it difficult, if not impossible, to be used by businesses having a large number of employees. For example, in a business of 1000 legitimate entities (e.g., employees), a maximum of 499,500 (1000×999/2) keys would need to be managed, provided that each legitimate entity is capable of communicating with any another legitimate entity within the business. In addition, symmetric key cryptography is difficult to implement in a network or global environment because there is no secure

and convenient way of transmitting the symmetric key from the legitimate sender **2** to the legitimate receiver **3**.

Another method of encryption/decryption is to use two separate keys (referred to as a "key pair") in which a first key ("a public key") **10** of the key pair is used for encryption of a message **12** from a legitimate sender **13** while a second key ("a private key") **11** of the key pair is used by the legitimate receiver **14** for decryption of the message **12** as shown in FIG. **2**. This method is commonly referred to as "asymmetric" (or public) key cryptography. One advantage of asymmetric key cryptography is that it alleviates the burdensome key management problem associated with symmetric key cryptography. Continuing the above example, the number of key pairs required for asymmetric key cryptography is equal to 1000, the total number of legitimate entities. However, in such communications system, it is known that an illegitimate entity (e.g., commercial spy) may attempt to impersonate a legitimate entity (e.g., employee, joint-venturer, etc.) by sending fraudulent messages to another legitimate entity for the purpose of disrupting work flow or obtaining confidential information. Thus, additional protocols are usually used in the asymmetric key system to ensure message and sender authentication.

Authentication of the sender (i.e., verifying that the sender of a public key is, in fact, the true owner of the public key) is a problem when communications are initially established between previously unknown parties. This problem is commonly avoided by incorporating a digital certificate **15** within the transmitted message **12** as shown in FIG. **3**. The digital certificate **15** is issued by a mutually trusted authority **16** (e.g., a bank, governmental entity, trade association, etc.) so that fraudulent attempts to use another's public key **10** will simply result in unreadable messages. Such mutually trusted authority **16** depends on the parties involved. For example, two individuals employed by the same business could both trust the certificates issued by a corporate security office of the business. Employees of two independent business entities, however, would require not only the certificates from the respective security offices, but also the certificates from, for example, some industry trade organization that certifies such business entities. This digital certificate **16** methodology "binds" a public key **10** to an entity (e.g., employee).

In the past few years, there have been many approaches toward protecting "key" information from being obtained by unauthorized persons. One such approach is employing mechanical security mechanisms, particular for portable computers which can be more easily appropriated. For example, certain companies have introduced a "secure" laptop using a tamper-detection mechanism to erase the key material if the laptop's casing is opened without authorization. However, there are several disadvantages associated with mechanical security devices.

A primary disadvantage associated with mechanical security mechanisms is that they may be circumvented through reverse engineering. Another disadvantage is that mechanical security mechanisms are costly to design and fabricate. Another disadvantage is that they are subject to accidental erasure of key information.

As a result, a number of companies are simply relying on the software application to utilize encryption/decryption protocols. However, as technology rapidly evolves, these encryption/decryption software applications place unnecessary limitations on transmission speeds of a communication system since the speed of encrypting or decrypting information is correlated to the execution speed of the instructions.

This approach for employing specific hardware into the customer's system to protect such keys from disclosure is also used in the rapidly growing area of "content distribution", namely the electronic distribution of information. Some known content distribution systems include (i) selling software via modem or other electronic means and (ii) selling portions of information distributed by compact disc ("CD"), etc. Such electronic sales often depend on the use of decryption keys to "decode" the specific data involved. For example, a customer may have free access to a CD containing many files of encrypted data, but to actually purchase a specific file, he buys the corresponding "decryption key" for that file. However, a primary problem with using specific hardware to protect the keys is that such hardware requires complete management and control by the information supplier to prevent any potential unauthorized uses.

BRIEF SUMMARY OF THE INVENTION

Based on the foregoing, it would be desirable to develop a semiconductor device comprising a processing unit for performing operations for identification purposes, a memory unit having at least non-volatile memory for storage of a unique public/private key pair and at least one digital certificate verifying the authenticity of the key pair, memory for storage of cryptographic algorithms and volatile random access memory for storage of temporary data. The hardware agent further includes an interface in order to receive information (encrypted or decrypted) from and/or transmit information to other device(s).

BRIEF DESCRIPTION OF THE DRAWINGS

The objects, features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

FIG. **1** is a block diagram illustrating a conventional symmetric key encryption and decryption process.

FIG. **2** is a block diagram illustrating a conventional asymmetric key encryption and decryption process.

FIG. **3** is a block diagram illustrating a digital certification process from a trusted authority.

FIG. **4** is a block diagram of a computer system incorporating an embodiment of the present invention.

FIG. **5** is a block diagram of an embodiment of the present invention.

FIG. **6** is a flowchart illustrating the method for implementing a key pair and digital certificate into a cryptographic semiconductor device.

FIG. **7** is a flowchart illustrating the operations of the hardware agent.

FIG. **8** is a flowchart illustrating remote verification of the hardware agent using second level certification.

DETAILED DESCRIPTION OF THE INVENTION

The present invention relates to a a cryptographic semiconductor device of many possible embodiments (referred to as a "hardware agent") and its associated method of operation directed toward securely storing and using a public/private key pair and at least one digital certificate within the hardware agent itself. This digital certificate may include a "device certificate" being a digital certificate provided by a manufacturer of the device signifying the legitimacy of the device, a "second level certificate" being a digital certificate from a trusted third party or a collection of both certificates. In the following description, numerous details are set forth such as certain components of the hardware agent in order to provide a thorough understanding of the present invention. It will be obvious, however, to one skilled in the art that these details are not required to practice the present invention. In other instances, well-known circuits, elements and the like are not set forth in detail in order to avoid unnecessarily obscuring the present invention.

Referring to FIG. **4**, an embodiment of a computer system **20** utilizing the present invention is illustrated. The computer system **20** comprises a system bus **21** enabling information to be communicated between a plurality of bus agents including at least one host processor **22** and a hardware agent **23**. The host processor **22**, preferably but not exclusively an Intel® Architecture Processor, is coupled to the system bus **21** through a processor bus interface **24**. Although only the host processor **22** is illustrated in this embodiment, it is contemplated that multiple processors could be employed within the computer system **20**.

As further shown in FIG. **4**, the system bus **21** provides access to a memory subsystem **25** and an input/output ("I/O") subsystem **26**. The memory subsystem **25** includes a memory controller **27** coupled to the system bus **21** to provide an interface for controlling access to at least one memory device **28** such as dynamic random access memory ("DRAM"), read only memory ("ROM"), video random access memory ("VRAM") and the like. The memory device **28** stores information and instructions for the host processor **22**.

The I/O subsystem **26** includes an I/O controller **29** being coupled to the system bus **21** and a conventional I/O bus **30**. The I/O controller **29** is an interface between the I/O bus **30** and the system bus **21** which provides a communication path (i.e., gateway) to allow devices on the system bus **21** or the I/O bus **30** to exchange information. The I/O bus **30** communicates information between at least one peripheral device in the computer system **20** including, but not limited to a display device **31** (e.g., cathode ray tube, liquid crystal display, etc.) for displaying images; an alphanumeric input device **32** (e.g., an alphanumeric keyboard, etc.) for communicating information and command selections to the host processor **22**; a cursor control device **33** (e.g., a mouse, trackball, etc.) for controlling cursor movement; a mass data storage device **34** (e.g., magnetic tapes, hard disk drive, floppy disk drive, etc.) for storing information and instructions; an information transceiver device **35** (fax machine, modem, scanner etc.) for transmitting information from the computer system **20** to another device and for receiving information from another device; and a hard copy device **36** (e.g., plotter, printer, etc.) for providing a tangible, visual representation of the information. It is contemplated that the computer system shown in FIG. **4** may employ some or all of these components or different components than those illustrated.

Referring now to an embodiment of the present invention as shown in FIG. **5**, the hardware agent **23** is coupled to the system bus **21** to establish a communication path with the host processor **22**. The hardware agent **23** comprises a single integrated circuit in the form of a die **40** (e.g., a microcontroller) encapsulated within a semiconductor device package **41**, preferably hermetically, to protect the die **40** from damage and harmful contaminants. The die **40** comprises a processing unit **42** coupled to a memory unit **43**, a bus interface **44** and a number generator **45**. The bus interface **44** enables communication from the hardware agent **23** to another device (e.g., the host processor **22**). The

processing unit **42** performs computations internally within a secured environment within the die **40** to confirm a valid connection with an authorized receiver. Such computations include executing certain algorithms and protocols, activating circuitry (e.g., the number generator **45** being preferably random in nature) for generating a device-specific public/private key pair and the like. The processing unit **42** is placed within the die **40** to prevent access of -the private key through virus attack, which is a common method of disrupting a computer system to obtain its private key.

The memory unit **43** includes a non-volatile memory element **46** which stores the public/private key pair and at least one digital certificate therein. This non-volatile memory **46** is used primarily because it retains its contents when supply power is discontinued. The memory unit **43** further includes random access memory ("RAM") **47** in order to store certain results from the processing unit **42** and appropriate algorithms.

Although the hardware agent **23** is implemented as a peripheral device on the system bus **21** for greater security, it is contemplated that the hardware agent **23** could be implemented in several other ways at the PC platform level such as, for example, as a disk controller or PCMCIA card to automatically decrypt and/or encrypt information being inputted and outputted from a hard disk. Another alternative implementation would be for the hardware agent **23** to be one component of a multi-chip module including the host processor **22** as discussed below. Furthermore, even though the hardware agent **23** is described in connection with PC platforms, it is contemplated that such hardware agent **23** could be implemented within any input/output ("I/O") peripheral device such as within a fax machine, printer and the like or on a communication path between a computer and the I/O peripheral device.

Referring to FIG. **6**, a flowchart of the operations for manufacturing the present invention is illustrated. First, in Step **100**, the die of the hardware agent is manufactured according to any conventional well-known semiconductor manufacturing technique. Next, the die is encapsulated within a semiconductor package so as to form the hardware agent itself (Step **105**). The hardware agent is placed onto a certification system which establishes an electrical connection to the hardware agent and the certification system (Step **110**). The certification system is basically a carrier coupled to a printed circuit board for generating and receiving electrical signals for certification of the hardware agent. The certification system includes a device for storage of prior generated public keys (e.g., a database) to guarantee unique key generation. Thereafter, the certification system supplies power to the hardware agent initiating a configuration sequence. During this sequence, the random number generator generates a device-specific public/private key pair internally within the hardware agent (Step **115**).

The public key of the public/private key pair is output to the certification system (Step **120**) where it is compared to the storage device of the prior generated public keys from previously manufactured hardware agents (Step **125**). In the highly unlikely event that the public key is identical to a prior generated public key (Step **130**), the hardware agent is signaled by the certification system to generate another such public/private key pair (Step **135**) and continue process at Step **120**. This process ensures that each public/private key pair is unique. The storage device for prior generated public keys is updated with this new, unique public key (Step **140**). Thereafter, in Step **145**, the certification system creates a unique device certificate by "digitally signing" the public key with the manufacturer's secret private key (i.e. in general terms, encrypting the public key with the manufacturer's private key). This certificate is input to the hardware agent (Step **150**) and the hardware agent permanently programs the unique public/private key pair and the device certificate into its non-volatile memory (Step **155**). At this point, the device is physically unique and is now capable of proving its authenticity.

Referring to FIG. **7**, a flowchart of remote verification of a hardware agent is illustrated. In Step **200**, a communication link is established between a system incorporating the hardware agent ("local system") and a remote system (e.g., a system incorporating another hardware agent or running software which communicates with the hardware agent). The hardware agent outputs its unique device certificate to the remote system (Step **205**). Since the manufacturer's public key will be published and widely available, the remote system decrypts the device certificate to obtain the public key of the hardware agent (Step **210**).

Thereafter, in Step **215**, the remote system generates a random challenge (i.e., a data sequence for testing purposes) and transmits the random challenge to the local system (Step **220**). In step **225**, the hardware agent generates a response (i.e., encrypts the challenge with the private key of the hardware agent) and transmits the response to the remote system (Step **230**). Then, the remote system decrypts the response with the public key of the hardware agent as previously determined from the device certificate transmitted by the hardware agent (Step **235**). In Step **240**, the remote system compares the original challenge to the decrypted response and if identical, communications between the system and the remote system are secure and maintained (Step **245**). Otherwise, the communications are terminated (step **250**). At this point, the remote system is ensured that it is in direct contact with a specific device (of known characteristics) manufactured by a specific manufacturer. The remote system can now direct the hardware agent to perform specific functions within the target system on the remote's behalf. The integrity of these functions and secrecy of the associated data are ensured. Such functions may include receipt and use of content distribution keys, maintenance of accounting information, etc.

With the emergence of content distribution along, with other information providing devices, it may become necessary to provide additional assurances that the hardware agent is not a forgery. This can be accomplished by sending the hardware agent to a reputable third party entity such as another trusted authority e.g., governmental agency, bank, trade association and the like. In a manner identical to that described above, a unique third party digital certificate of the third party entity (the "second level certificate") is input to the hardware agent. Thereafter, the hardware agent permanently programs the second level certificate accompanied by the public/private key pair and possibly the device certificate into its non-volatile memory. As a result, the hardware agent is validated through both the device certificate and the second level certificate to guarantee validity of the hardware agent and prevent fraudulent manufacture of the hardware agent, barring unlikely collusion by the third party entity and the manufacturer of the hardware agent.

Referring to FIG. **8**, a flowchart of remote verification of a hardware agent including authentication using a second level certificate is illustrated. In Step **300**, a communication link is established between the local system and the remote system. The hardware agent outputs its unique device certificate and the second level certificate to the remote system (Step **305**). Next, the remote system decrypts the device certificate using the manufacturer's published public key to

obtain the public key of the hardware agent (Step **310**). Similarly, the remote system decrypts the second level certificate using a well-published public key of the third party to obtain the public key of the hardware agent stored therein (Step **315**).

Thereafter, the two versions of the public key of the hardware agent are compared (step **320**) and if the two versions are not identical, communication is terminated (Step **325**). However, if the two versions are identical, the remote system generates a random challenge and transmits the random challenge to the hardware agent (Step **330**). The hardware agent generates a response i.e., the challenge encrypted with the private key of the hardware agent (Step **335**) and transmits the response to the remote system (Step **340**). The remote system then decrypts the response with the public key of the hardware agent previously transmitted by the hardware agent (Step **345**). As in Step **350**, the remote system compares the original challenge to the decrypted response and if identical, communications between the system and the remote system are secure and maintained (Step **355**). Otherwise, the communications are terminated (step **360**).

The present invention described herein may be designed in many different methods and using many different configurations. While the present invention has been described in terms of various embodiments, other embodiments may come to mind to those skilled in the art without departing from the spirit and scope of the present invention. The invention should, therefore, be measured in terms of the claims which follows.

What is claimed is:

1. A semiconductor device comprising:

processing means for processing information within said semiconductor device;

first storage means for storing a uniquely designated key pair and at least one digital certificate, said first storage means being coupled to said processing means;

second storage means for storing at least said information processed by said processing means, said second storage means being coupled to said processing means; and

generating means for generating values used to produce at least one key internally within the semiconductor device, said generating means being coupled to said processing means.

2. The semiconductor device according to claim **1**, wherein said first storage means includes non-volatile memory for maintaining said uniquely designated key pair and said at least one digital certificate even during a non-powered state.

3. The semiconductor device according to claim **2**, wherein said at least one digital certificate includes a device certificate.

4. The semiconductor device according to claim **3**, wherein said at least one digital certificate further includes a second level certificate.

5. The semiconductor device according to claim **2**, wherein said second storage means includes random access memory for temporarily storing said information.

6. The semiconductor device according to claim **1**, wherein said generating means includes a random number generator.

7. The semiconductor device according to claim **1** wherein said further comprising interface means for providing a mechanism to couple the semiconductor device to a communication link.

8. The semiconductor device of claim **1**, wherein the at least one key includes the key pair.

9. A system comprising:

memory means for storing program instructions;

host processing means for executing said program instructions;

bus means for coupling said host processing means and said memory means; and

semiconductor means, coupled to said bus means, for internally decrypting input information and encrypting output information, said semiconductor means including:

processing means for processing said input and output information within said semiconductor means,

first storage means for storing a uniquely designated key pair and at least one digital certificate used for decrypting said input information and encrypting said output information, said first storage means being coupled to said processing means,

second storage means for temporarily storing at least said input and output information, and

generating means for generating values used to produce at least one key internally within the semiconductor means.

10. The system according to claim **9**, wherein said first storage means includes non-volatile memory for storing said uniquely designated key pair and said at least one digital certificate during a non-powered state.

11. The system according to claim **10**, wherein said at least one digital certificate includes a device certificate.

12. The system according to claim **11**, wherein said at least one digital certificate further includes a second level certificate.

13. The system according to claim **10**, wherein said second storage means includes random access memory for temporarily storing said information and at least one encryption and decryption algorithm.

14. The system according to claim **9**, wherein said generating means includes a random number generator.

15. The system of claim **9**, wherein the at least one key includes the key pair.

16. A semiconductor device for performing cryptographic operations, said semiconductor device comprising:

a first memory element for containing at least a designated key pair and at least one digital certificate;

a second memory element for containing information;

a processing unit coupled to said first and second memory elements, said processing unit for processing said information; and

a random number generator coupled to said processing unit, said random number generator for generating values which are used to generate at least one key internally within the semiconductor device.

17. The semiconductor device according to claim **16**, wherein said first memory element is non-volatile memory.

18. The semiconductor device according to claim **17**, wherein said second memory element is volatile memory.

19. The system according to claim **17**, wherein said designated key pair is unique.

20. The semiconductor device according to claim **16**, wherein said first memory element contains a device certificate and a second level certificate.

21. The semiconductor device of claim **16**, wherein the at least one key includes the key pair.

22. A system comprising:

a bus;

a memory element containing program instructions and data;

a host processor coupled to said bus, said host processor executes said program instructions;

a semiconductor device coupled to said bus, said semiconductor device internally encrypting output information to be sent to a remote system remotely located from the system, said semiconductor device including

a first memory element which contains a designated key pair and at least one digital certificate,

a second memory element which contains information,

a processing unit coupled to said first and second memory elements, said processing unit processing at least said information, and

a random number generator coupled to aid processing unit, said random number generator generating values which are used to generate at least one key internally within said semiconductor device.

23. The system according to claim **22**, wherein said first memory element of said semiconductor device includes non-volatile memory.

24. The system according to claim **23**, wherein said second memory element of said semiconductor device includes non-volatile memory.

25. The system according to claim **22**, wherein said semiconductor device and said host processor are encapsulated within as a multi-chip package.

26. The system according to claim **22** further comprising an information transceiver device coupled to at least said semiconductor device.

27. The system according to claim **26**, wherein said information transceiver device is one of a group consisting of a modem or a fax machine.

28. The system according to claim **26**, wherein said information transceiver device is also coupled to one of a group consisting of a network or a telephone line, said information transceiver device enables information to be exchanged with the remote system.

29. The system of claim **22**, wherein the at least one key includes the key pair.

* * * * *